REMARKS

Initially, Applicant notes that the remarks and amendments made by this paper are consistent with the proposals presented to the Examiner during the telephone call of October 4, 2007 and which appear to overcome all of the rejections of record for at least the reasons presented over the phone.

The Final Office Action, mailed September 5, 2007, considered and rejected claims 1-36. Claims 1-7, 15, 19-21, 25-29 and 34 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Jackson et al. (US 7,116,782), hereinafter Jackson, in view of Ault et al. (US 6,377,994), hereinafter Ault. Claims 8-13, 16-18, 22-24, 30-33 and 35-36 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Jackson et al. (US 7,116,782) and Ault et al. (US 6,377,994) as applied to claim 5, and further in view of Musgrave et al. (US 6,202,151), hereinafter Musgrave.

By this response, claims 1-2, 5, 8-11, 14, 19-24, and 27-33 have been amended, claims 3-4, 6-7, 9-10,12-13, 15-18, 25-26, and 34-36 have been canceled and no claims have been added, such that claims 1-2, 5, 8, 11, 14, 19-24, and 27-33 remain pending, of which claims 1, 19, 20, and 27 are the only independent claims at issue. [1]

With regard to the objections of claims 1 and 3, it will be noted that claim 1 has been amended to include the Examiners recommendation, while claim 3 has been canceled, rendering the objection to it moot. The rejection of claims 1-19 is now obviated in light of the amendment to claim 1. Specifically claim 1 has been amended to clarify that the key is used to generate a temporary signature based on the stored data, rather than stating that the signature is generated using the key as well as the stored data.

The pending claims are currently directed to embodiments for ensuring that data stored by an untrusted entity is not in an altered state when it is subsequently accessed. Claim 1, for example, recites a method for ensuring that data stored in a persistent storage of an untrusted entity by the untrusted entity have not been modified when the data are subsequently accessed for use by the untrusted entity. The method comprises the steps sending data related information to a trusted entity to compute a signature of the data. The trusted entity employs a key that is

[1] Support for the claim amendments is found throughout the Specification and more particularly on page 14 of the Application as originally filed. Accordingly, Applicant respectfully submits that the claim amendments do not add new manner, and entry thereof is respectfully requested.

only known and available for use by a trusted entity to compute a signature for the data related information before the data are stored in the persistent storage by the untrusted entity. The trusted entity then sends the signature to the untrusted entity and the signature and the data are then stored in the persistent storage of the untrusted entity. Before the stored data are subsequently used by the untrusted entity, the unaltered state of the data is verified by sending the data related information back to the trusted entity for verification. The trusted entity utilizes the key that is only known and available for use by the trusted entity to generate a temporary signature based on the stored data that is compared with the stored signature. The stored data are then only used by untrusted entity if the step of verifying indicates that the data that were stored have not been changed since the signature was computed before storing the data.

The remaining independent claims are closely related to claim 1. Claim 19 recites a computer program product corresponding to claim 1, while claims 20 and 27 are directed to embodiment for systems performing methods similar to claim 1 from the perspective of an untrusted entity and a trusted entity, respectively.

Applicant notes that while Jackson and Ault appear to disclose embodiments for using a key to securely sign data on an untrusted entity, the combined references do not disclose various features of the present invention. In contrast to Applicant's claimed invention, for example, Jackson does not disclose any embodiment wherein that would include the use of unpaired keys, the trusted entity doing all signature calculations, or the untrusted entity sending data-related information to the trusted entity. Ault also fails to teach or suggest these limitations.

In the office action, Examiner has relied upon Ault, and apparently an assertion in Applicants' Specification, to assert that a client and server are interchangeable. While this may be true in some circumstances, the interchangeability of claim limitations between acts performed by the client and the server are not interchangeable per se. Instead, the relationship between the client and server must still be preserved. To help clarify this relationship, Applicant has amended the claims to no longer reference a client and server, but and instead to indicate a trusted and an untrusted entity relationship. As such, the two entities are not interchangeable and the teachings of Ault are not applicable. Furthermore, Applicant respectfully disagrees with the assertion that the use of client and server are interchangeable within the embodiments, per se. The referenced portion of the Specification indicates that the terms client and server are relative and can be readily switched, but this does not indicate interchangeability within the claims

themselves and particularly within the claim elements, at any random time. Even more particularly, a client computing system can sometimes operate as a server to another computer, such that the client and server terminology can be switched, but only for the claim as a whole and not for individual elements within the claim.

The referenced disclosure of Jackson fails to fully teach the embodiments of claim 1. For example, fig. 3 shows only a method for creating a digital signature using public and private keys. The present claims, on the other hand, do not utilize key pairs. Instead the computation of signatures is always done at the server, even the computation of the signature for the previously stored data. Instead, Jackson teaches only the use of private/public key pairs for the signing of data. As stated in the background of the Application, the present embodiments are advantageous for the reason that they do not require shared keys as is the normal procedure for data encryption.

Additionally, the current claims require the untrusted entity to send the data related information to the trusted entity for computation of the signature. The disclosure of Jackson only discloses the trusted entity sending the signature and the data to the untrusted entity. Jackson does not ever disclose the untrusted entity sending the data back to the trusted entity to compute a signature. Yet another limitation is found in claim 1 (but not the related system claims) wherein the data is generated by the untrusted entity for subsequent key generation. This limitation is not disclosed within Jackson as Jackson only discloses data that is pushed to the untrusted entity.

While only the specific limitations of claim 1 have been discussed, independent claims 19, 20, and 27 were rejected using the same rationale as claim 1 and the above arguments are therefore appropriate for those claims as well. It will be appreciated that because the all of the independent claims have been addressed, each dependent claim is allowable over the cited art for at least the same reasons, and the other rejections and assertions of record with respect to the other dependent claims are now moot, and therefore need not be addressed individually. Nevertheless, to further differentiate between the cited references and the present invention, dependent claims 8, 11, 22, 23, 30, and 32 and their associated dependent claims will be addressed.

With respect to claim 8, the method further includes obtaining a signer identification (ID) for the untrusted entity, wherein the ID uniquely identifies the untrusted entity and not being controlled by the operator of the untrusted entity. The examiner has acknowledged that such a

feature is not present in the teaching or suggesting of Jackson and Ault. To demonstrate this feature, the Examiner relies on Musgrave. However, Applicant respectfully disagrees with the conclusion that Musgrave teaches the limitations of claim 8. Specifically, Musgrave does not teach or suggest the required limitation of the ID uniquely identifying the untrusted entity rather than the operator of the device. Instead, Musgrave discloses a technique for combining biometric identification with digital certificates for electronic authentication called biometric certificates and for obtaining the identification of the operator (not the untrusted entity). It is disclosed in Musgrave that biometric data includes genetic composition, fingerprints, hand geometry, iris and retinal appearance, etc. All of these features are clearly user related, not device dependent. Because claims 11, 16, 22, 23, 30, 32 and 35 all contain the same language limiting the ID to the client device, they are allowable for at least the same reasons articulated for claim 8.

In view of the foregoing, Applicant respectfully submits that the other rejections to the claims are now moot and such that any of the remaining rejections and assertions made, particularly with respect to all of the dependent claims, do not need to be addressed individually at this time. It will be appreciated, however, that this should not be construed as Applicant acquiescing to any of the purported teachings or assertions made in the last action regarding the cited art or the pending application, including any official notice, and particularly with regard to the dependent claims.[2]

[2] Instead, Applicant reserves the right to challenge any of the purported teachings or assertions made in the last action at any appropriate time in the future, should the need arise. Furthermore, to the extent that the Examiner has relied on any Official Notice, explicitly or implicitly, Applicant specifically requests that the Examiner provide references supporting any official notice taken. Furthermore, although the prior art status of the cited art is not being challenged at this time, Applicant reserves the right to challenge the prior art status of the cited art at any appropriate time, should it arise. Accordingly, any arguments and amendments made herein should not be construed as acquiescing to any prior art status of the cited art.

In the event that the Examiner finds remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney at 801-533-9800.

Dated this 10th day of October, 2007.

Respectfully submitted,

RICK D. NYDEGGER
Registration No. 28,651
JENS C. JENKINS
Registration No. 44,803
JOHN C. BACOCH
Registration No. 59,890
Attorneys for Applicant
Customer No. 47973

JCJ:ahy
AHY0000006260V001